

Upgrade von Access Point-Images für Remote-Bereitstellungen

Inhalt

[Einleitung](#)

[Upgrade-Methoden für Cisco Access Point-Images](#)

[Die Herausforderung: Herunterladen von Standard-CAPWAP-Images über WAN](#)

[Verbessertes CAPWAP-Image-Download-Fenster](#)

[Prozessübersicht](#)

[Konfiguration \(CLI\)](#)

[Überprüfung \(CLI\)](#)

[Einschränkungen/Überlegungen](#)

[Effizientes Image-Upgrade im FlexConnect-Modus](#)

[Prozessübersicht](#)

[Vorteile](#)

[Konfiguration \(CLI\)](#)

[Überprüfung \(CLI\)](#)

[Einschränkungen/Überlegungen](#)

[Download von HTTP-basierten AP-Images für Out-of-Band](#)

[Anwendungsfall](#)

[Prozessübersicht](#)

[Konfiguration \(CLI\)](#)

[Konfiguration \(GUI\)](#)

[Überprüfung \(CLI\)](#)

[Einschränkungen/Überlegungen](#)

[Manuelles, individuelles AP-Upgrade über TFTP/SFTP](#)

[Prozessübersicht](#)

[Konfiguration \(AP-CLI\)](#)

[Verifizierung](#)

[Einschränkungen/Überlegungen](#)

[Welche Methode für welche verwenden](#)

[Schlussfolgerung](#)

[Referenzen](#)

Einleitung

In diesem Dokument werden Methoden für effiziente Cisco AP-Image-Upgrades über WANs beschrieben, um Latenz- und Zuverlässigkeitsprobleme zu lösen.

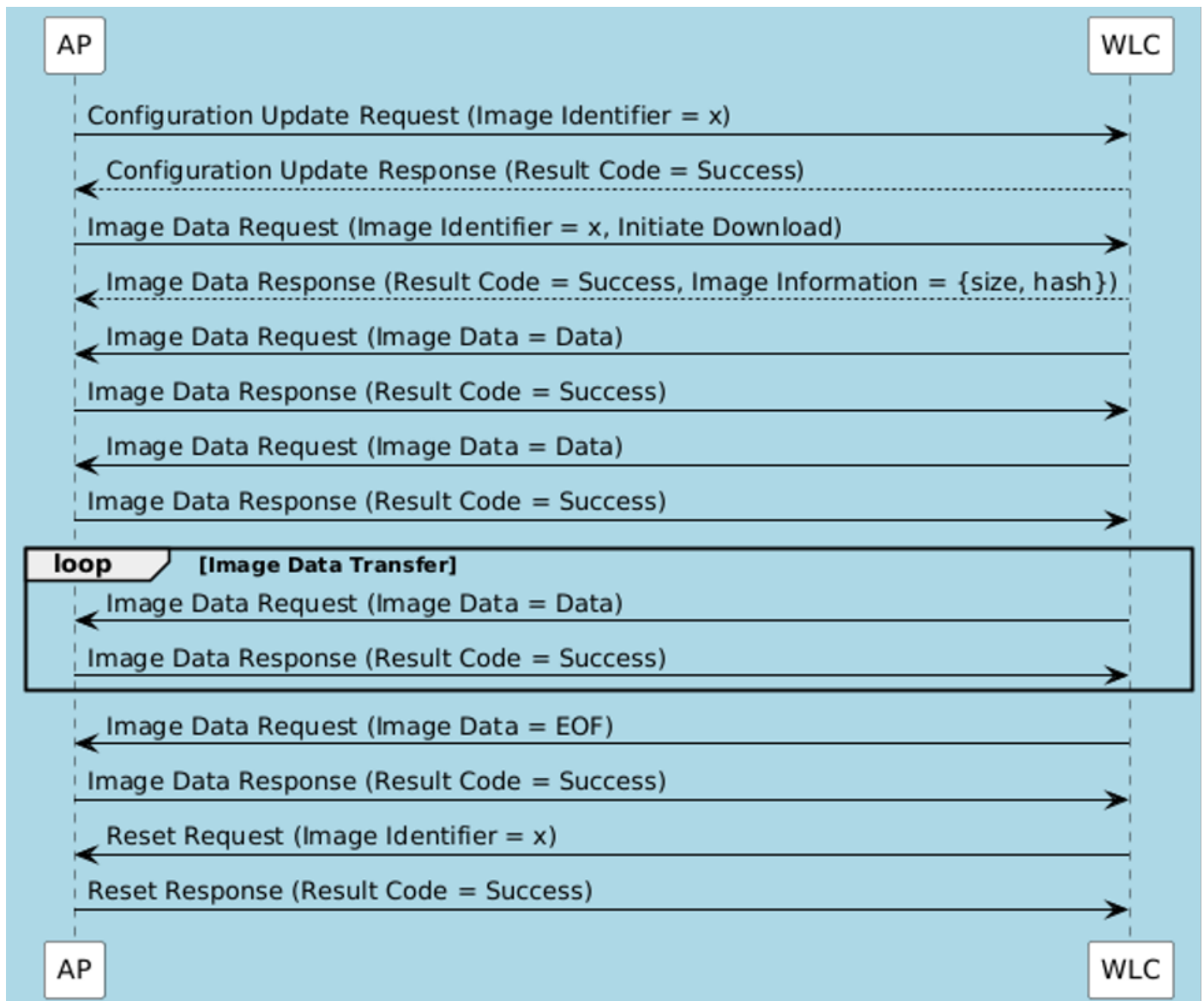
Upgrade-Methoden für Cisco Access Point-Images

Regelmäßige Image-Upgrades sind für Cisco Access Points (APs) unerlässlich. Die Durchführung dieser Upgrades über WAN-Verbindungen (Wide Area Network) mit hoher Latenz kann jedoch eine Herausforderung darstellen. Die standardmäßige CAPWAP-Methode zum Herunterladen von Images ist zwar in lokalen Netzwerken effektiv, kann jedoch langsam sein und in Bezug auf WANs weniger zuverlässig sein. In diesem Abschnitt wird untersucht, warum dies der Fall ist, und es werden alternative und verbesserte Methoden beschrieben, die für effiziente Remote-Upgrades entwickelt wurden.

Die Herausforderung: Herunterladen von Standard-CAPWAP-Images über WAN

Der grundlegende Prozess für das Upgrade des AP-Images über CAPWAP ist in [RFC 5415](#), Abschnitt 9.1 definiert. Dieser Mechanismus ermöglicht es dem Wireless LAN Controller (WLC), das neue AP-Image über den CAPWAP-Tunnel direkt an die angeschlossenen APs zu senden. Für jede Image Data Request Message (RFC 5415, Abschnitt 9.1.1), die einen Teil von Firmware-Daten enthält, wartet der WLC auf eine entsprechende Image Data Response Quittung (RFC 5415, Abschnitt 9.1.2) vom AP, bevor der nächste Teil gesendet wird.

Das Bild zeigt den Bildübertragungsprozess zwischen dem Access Point und dem WLC, während sich der Access Point im Ausführungszustand befindet.



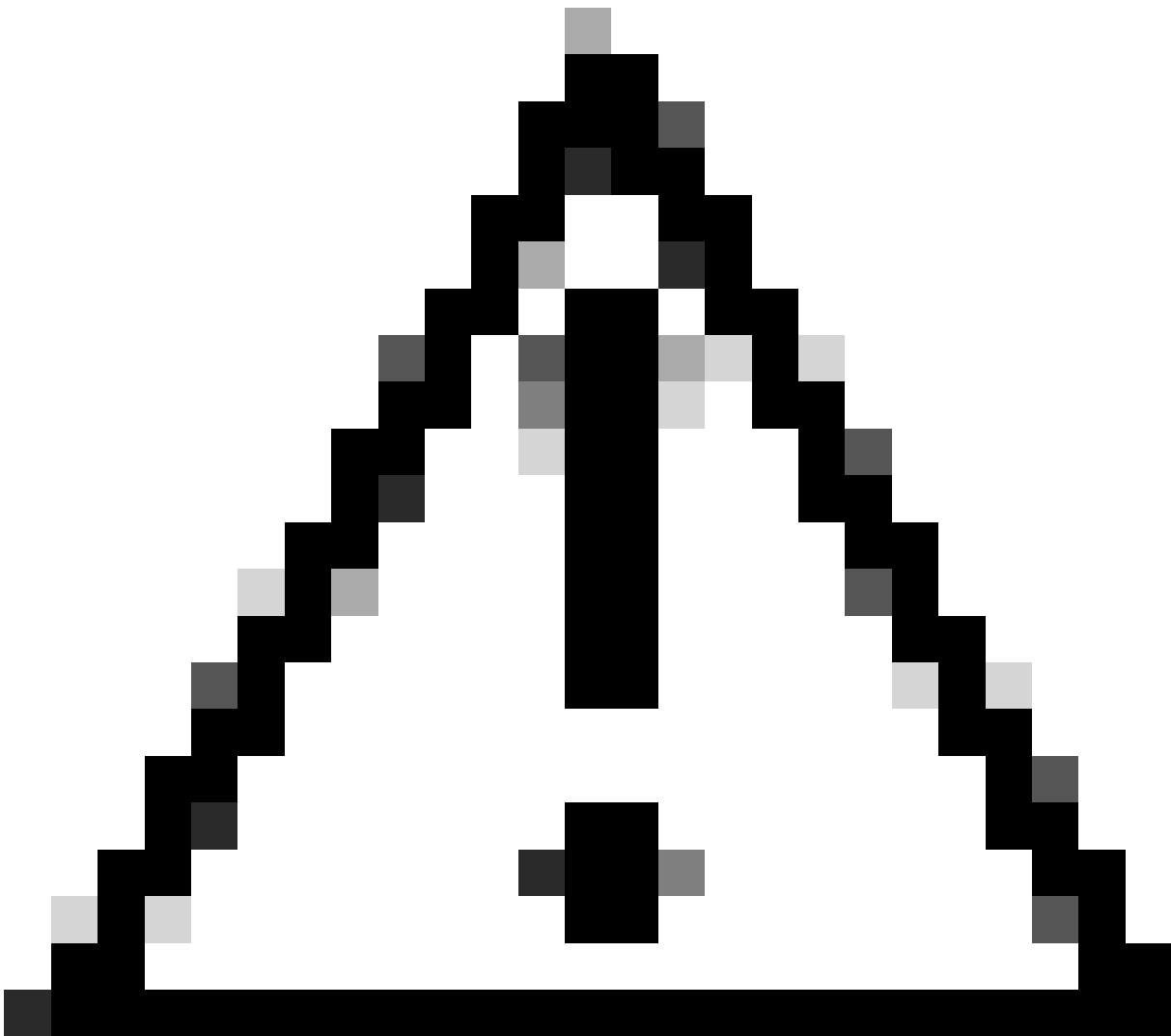
Prozessablauf bei AP-Image-Übertragung

Wie beobachtet, sendet der WLC Image Data Request-Nachrichten, die Teile der Firmware-Image-Daten enthalten. Der WAP bestätigt den Empfang dieser Blöcke durch Senden von Image Data Response-Nachrichten. Dieser Austausch wird fortgesetzt, bis das gesamte Bild übertragen wird.

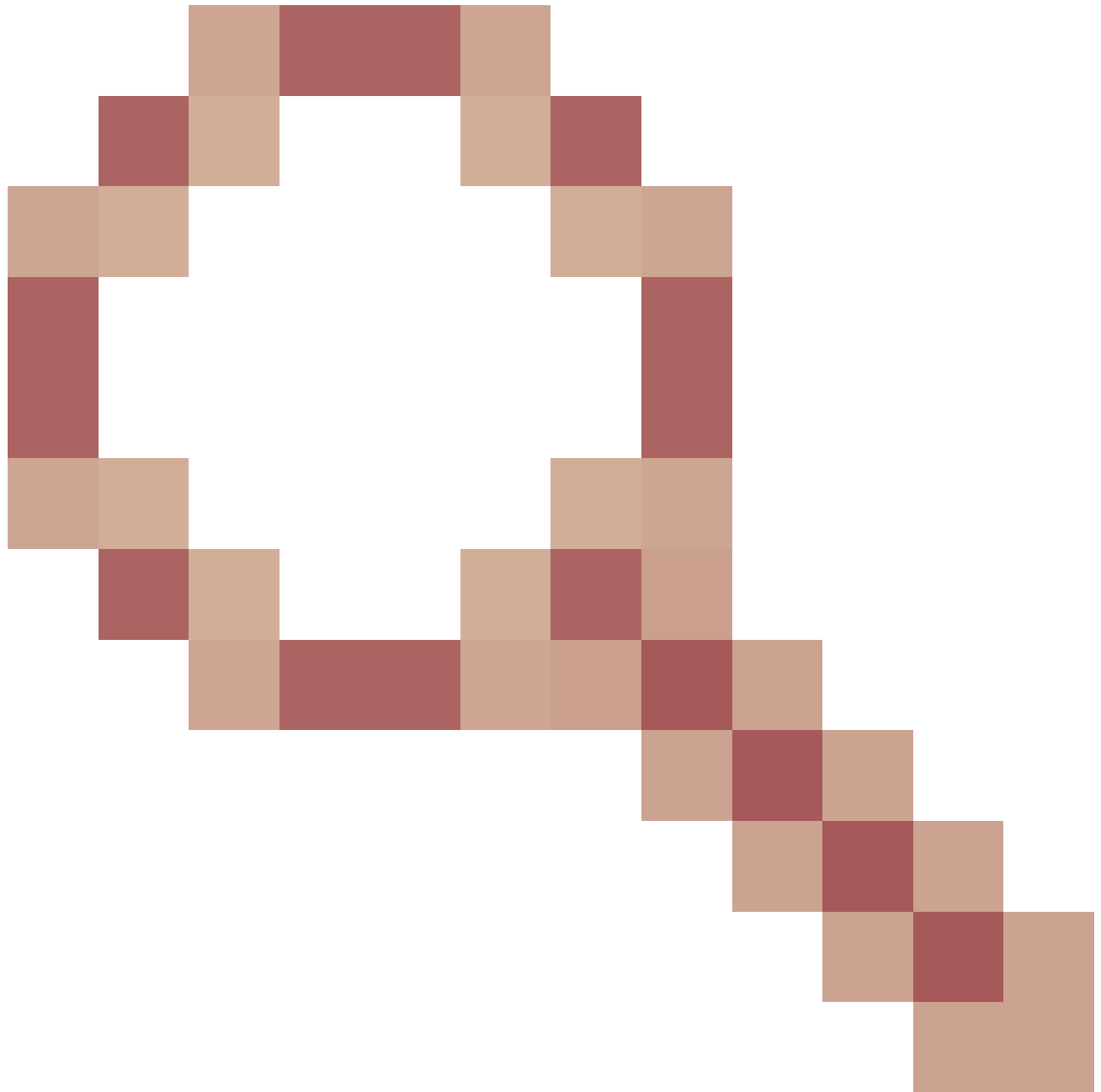
Für jede Image Data Request-Nachricht wird eine entsprechende Image Data Response-Nachricht als Quittung erwartet. Das bedeutet, dass der Access Point auf das Eintreffen der einzelnen Bildpakete warten, diese bestätigen und dann auf das nächste Paket warten muss. Dadurch wird der Download von Images in WAN-Umgebungen verlangsamt.

Hier ein Beispiel: Wenn die Round-Trip-Zeit (Round Trip Time, RTT) zwischen dem AP und dem WLC 100 ms beträgt, wird die Übertragungsrate auf ca. 10 Pakete pro Sekunde beschränkt. Wenn jede Paketgröße 1000 Byte beträgt, entspricht dies einem maximalen Durchsatz von 10 KB/s. Wenn das AP-Image 50 MB groß ist, beträgt die theoretische Minstdauer für die Übertragung ca. 5120 Sekunden. Dies zeigt, dass selbst bei Verfügbarkeit einer beträchtlichen Bandbreite der CAPWAP-Image-Download aufgrund dieses Stopp-and-Wait-Bestätigungsmechanismus langsam sein kann. Dieser Effekt tritt bei lokalen Image-Übertragungen, bei denen WLC und AP Teil

desselben Campus-Netzwerks sind und die Latenz minimal ist, weniger deutlich auf.



Vorsicht: Eine verlustbehaftete WAN-Verbindung kann zu Bildbeschädigungen führen.
Siehe Cisco Bug [ID CSCwf09053](#)



für weitere Informationen hierzu.

Um diese Einschränkungen des standardmäßigen CAPWAP-Kontrollpfad-Übertragungsmechanismus zu beseitigen, insbesondere in WAN-Umgebungen mit hoher Latenz oder eingeschränkter Bandbreite, wurden drei Verbesserungen eingeführt.

1. Die CAPWAP Window-Erweiterung verbessert den CAPWAP-Steuerpfad selbst durch die Implementierung eines Multi-Packet-Gleitfensters, das das Senden mehrerer Datenpakete ermöglicht, bevor eine Bestätigung erforderlich ist, wodurch der Durchsatz über Verbindungen mit hoher Latenz innerhalb des CAPWAP-Frameworks erhöht wird.
2. Efficient Image Upgrade im FlexConnect-Modus ist ein optimiertes Verfahren, das speziell für FlexConnect APs entwickelt wurde, die häufig in Zweigstellen mit begrenzter WAN-Bandbreite bereitgestellt werden. Diese Methode minimiert die WAN-Last, indem die Image-Download-Aufgabe verteilt wird.
3. Die Out-of-Band HTTPs-Based AP Image Download-Methode löst dies, indem ein

separates, effizienteres HTTPs-Protokoll verwendet wird, das auf einem dedizierten Webserver auf dem Controller für die Bildübertragung ausgeführt wird und außerhalb des restriktiven CAPWAP-Steuertunnels verschoben wird.

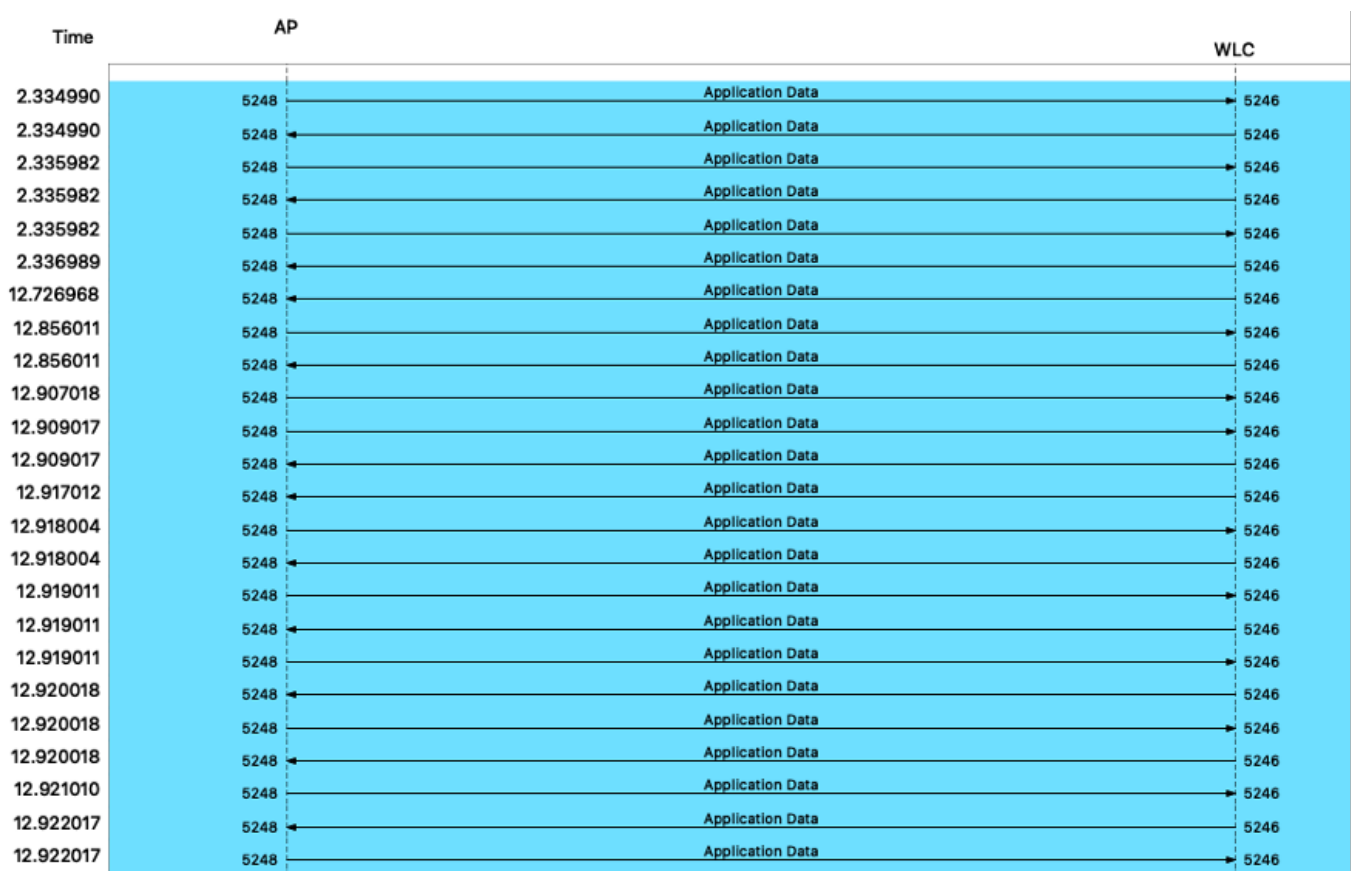
Verbessertes CAPWAP-Image-Download-Fenster

Diese Funktion erhöht die Geschwindigkeit beim Herunterladen von CAPWAP-basierten Images, die speziell für Office Extend Access Points (OEAP) oder Telearbeiter-APs entwickelt wurden. Es wird die Beschränkung des standardmäßigen CAPWAP-Steuerkanals mit einem einzigen Fenster angegangen, das vor dem Senden des nächsten Pakets eine Bestätigung für jedes Paket erfordert, wodurch Übertragungen über Verbindungen mit hoher Latenz verlangsamt werden. Diese Erweiterung unterstützt mehrere Schieberegler für Steuerungspakete.

Auswirkungen der CAPWAP-Fenstergröße

Die Effizienz des CAPWAP-Image-Download-Prozesses über den Steuerungskanal wird durch die konfigurierte Fenstergröße, insbesondere bei Verbindungen mit hoher Latenz, erheblich beeinflusst.

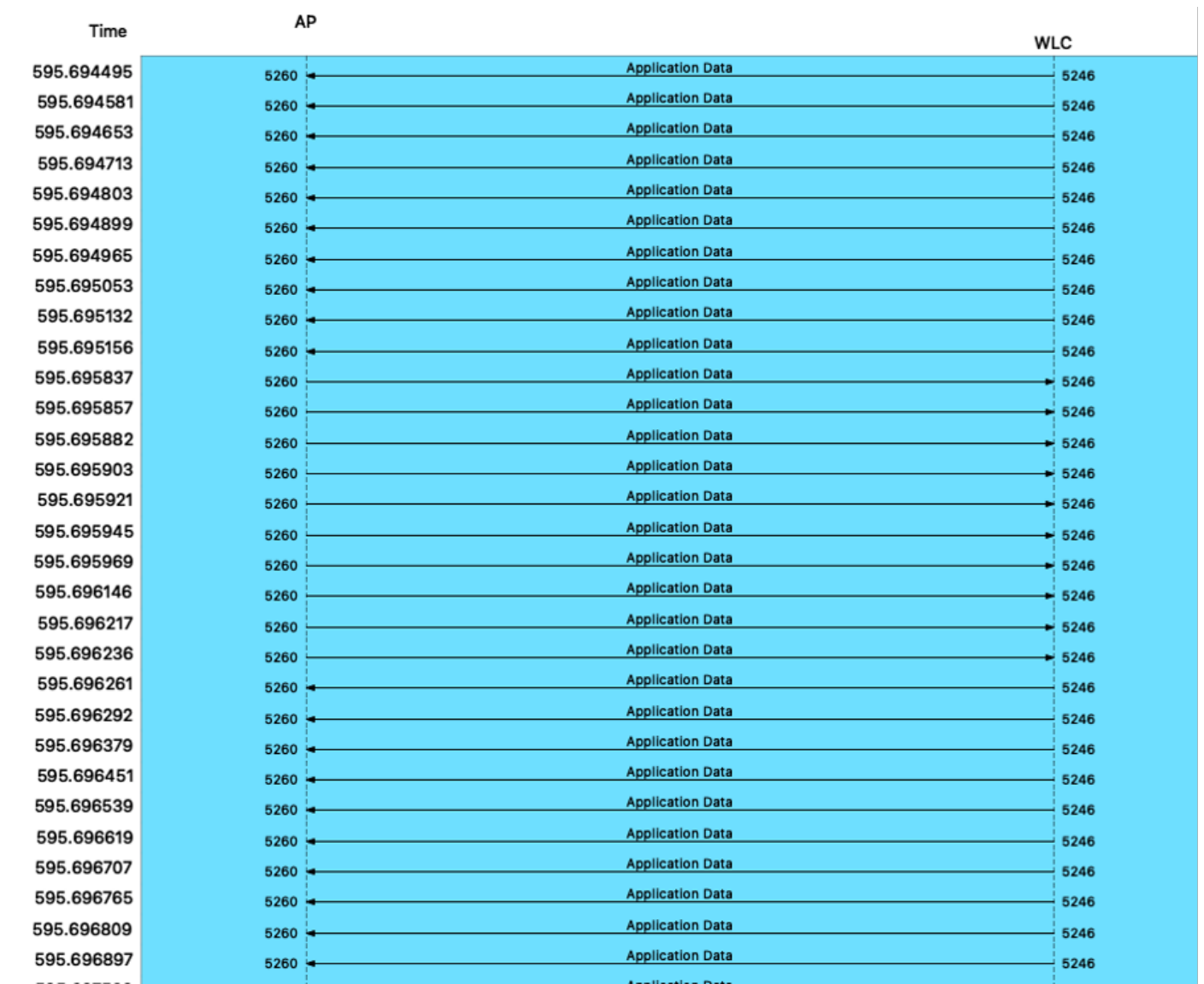
Bei CAPWAP-Fenstergröße = 1 (Standard/Standard): Der Paketfluss zeigt ein striktes Stopp-and-Wait-Verhalten. Für jedes vom WLC gesendete Bilddatenanforderungspaket hält der WLC an und wartet auf eine Bilddatenantwortbestätigung vom WAP, bevor das nächste Paket gesendet wird.



Aktualisierungsablauf des CAPWAP-Images mit Fenstergröße 1

Mit CAPWAP Window Size = N (z.B. 20): Der Paketfluss veranschaulicht einen

Gleitfenstermechanismus. Da mehrere Pakete über die Verbindung übertragen werden können, bevor eine Bestätigung erforderlich ist, wird die Latenz durch das Schiebfenster effektiv verdeckt.



Aktualisierungsablauf des CAPWAP-Images mit Fenstergröße 20

Prozessübersicht

1. Konfigurieren Sie ein AP-Profil speziell für OEAP/Telearbeiter-APs.
2. Legen Sie in diesem Profil eine CAPWAP-Fenstergröße größer als 1 fest.
3. Ordnen Sie dieses AP-Profil den OEAP-/Telearbeiter-APs zu.
4. Beim AP-Join-Vorgang wird die konfigurierte Fenstergröße angewendet.
5. Nachfolgende CAPWAP-Image-Downloads nutzen die größere Fenstergröße und verbessern so den Durchsatz.

Konfiguration (CLI)

Konfigurieren eines AP-Profiles und Festlegen der CAPWAP-Fenstergröße:

<#root>

```
configure terminal ap-profile capwap window size
```

```
<- Between 3 to 20
```

```
end
```

Ordnen Sie das AP-Profil einem Site-Tag zu, und wenden Sie es auf APs an (ähnlich wie in den Schritten 2 und 3 unter "Effizientes Image-Upgrade", um sicherzustellen, dass das richtige AP-Profil über das Site-Tag verknüpft wird).

Überprüfung (CLI)

```
<#root>
```

```
show ap profile name detailed
```

```
| in indo <- View CAPWAP window size in an AP profile
```

```
show capwap client rcb
```

```
| in Window <- View CAPWAP status and modes for a specific AP(Look for CAPWAP Sliding Window and Active)
```

```
show ap config general
```

```
| in indo <- View AP configuration details(Shows Capwap Active Window Size)
```

Einschränkungen/Überlegungen

- Diese Erweiterung wird nur auf OEAP-Profilen unterstützt.
- Die Fenstergröße wird auf dem Access Point nur während des AP-Join-Prozesses aktualisiert.
- Der Vorabdownload wird nicht ausgelöst, wenn das neueste Upgrade-Image bereits auf dem Access Point vorhanden ist.

Effizientes Image-Upgrade im FlexConnect-Modus

Efficient Image Upgrade ist ein optimiertes Verfahren, das speziell für FlexConnect-APs entwickelt wurde und insbesondere für Bereitstellungen in Zweigstellen mit begrenzter WAN-Bandbreite nützlich ist. Diese Methode minimiert die WAN-Last, indem ein primärer WAP innerhalb eines Standort-Tags festgelegt wird, um das Image vom Controller herunterzuladen. Anschließend können andere untergeordnete WAPs innerhalb desselben Standort-Tags das Image vom primären WAP über TFTP herunterladen. Der primäre Access Point ist ein Access Point pro Modell und Site-Tag.

Prozessübersicht

1. Ein neues AP-Image wird auf dem WLC bereitgestellt.
2. FlexConnect-APs werden einer Site-Tag-Nummer zugewiesen, die für ein effizientes Image-Upgrade konfiguriert wurde.
3. Der WLC wählt einen Access Point pro Modell innerhalb der Site-Tag-Nummer als primären Access Point aus.
4. Der primäre AP lädt das Image vom WLC über die WAN-Verbindung herunter (in der Regel über CAPWAP).
5. Wenn der primäre AP über das Image verfügt, laden untergeordnete APs mit demselben Site-Tag das Image vom primären AP über TFTP über das lokale Netzwerk herunter.
6. Maximal drei untergeordnete APs können gleichzeitig von einem primären AP heruntergeladen werden.
7. Nach dem Download laden die APs neu, um das neue Image auszuführen.

Vorteile

- Reduziert die WAN-Bandbreitennutzung, indem nur der primäre WAP das Image über das WAN herunterlädt.
- Nutzt schnellere lokale Netzwerkverbindungen (über TFTP) für die Image-Verteilung an untergeordnete APs.

Konfiguration (CLI)

<#root>

Enable Predownload in Flex Profile:

```
configure terminal
wireless profile flex
```

predownload

<- Enables the Efficient Image Upgrade option.

end

Configure a Site Tag and Associate Flex Profile:

```
configure terminal
wireless tag site
```

flex-profile

<- Ensure 'no local-site' is configured if not already, for Flexconnect mode
end

Attach Policy Tag and Site Tag to AP(s):

configure terminal
ap

<- Use wired MAC address
policy-tag

site-tag

rf-tag

end

Trigger Predownload to a Site Tag:

enable

ap image predownload site-tag

start

Überprüfung (CLI)

<#root>

show ap primary list

<- Display list of primary APs

show ap image

<- Display predownload status of APs: (Initially shows 'Predownloading', then 'Complete')

show ap name

image

<- Display image details for a specific AP

show capwap client rcb

<- Check if Flex efficient image upgrade is enabled on the AP console

Einschränkungen/Überlegungen

- Die über eine Standort-Tag-Nummer verbundenen APs müssen sich am selben physischen Standort befinden, um eine effiziente lokale TFTP-Übertragung zu ermöglichen.
- Verwendet den TCP-Port 8443 für den Listener-Service (wird auch für andere Funktionen wie Client-Debug-Pakete und CleanAir-Dateien verwendet). Dieser Port bleibt auch dann geöffnet, wenn die Funktion deaktiviert ist.
- Erfordert, dass sich der WLC im Installationsmodus befindet.

Download von HTTP-basierten AP-Images für Out-of-Band

Der HTTP-basierte OOB AP-Image-Download ist eine in Cisco IOS® XE Dublin 17.11.1 eingeführte verbesserte Methode zur Verbesserung der AP-Image-Upgrade-Leistung durch die Übertragung von Images außerhalb des standardmäßigen CAPWAP-Steuerpfads.

Die OOB-HTTPs-Methode nutzt das Standard-TCP und die HTTPs für die Bildübertragung. Im Gegensatz zum Stopp-and-Wait-Mechanismus des CAPWAP-Steuerungskanal verwendet TCP einen Gleitfenstermechanismus, der eine effiziente Massendatenübertragung über Verbindungen mit hoher Latenz ermöglicht.

Diese Methode verwendet einen Webserver (nginx), der auf dem Controller ausgeführt wird, um AP-Images über HTTPs direkt an die APs zu senden. Dadurch werden die Beschränkungen des CAPWAP-Steuerpfads für große Dateiübertragungen umgangen und ein potenziell schnellerer und flexiblerer Downloadmechanismus ermöglicht.

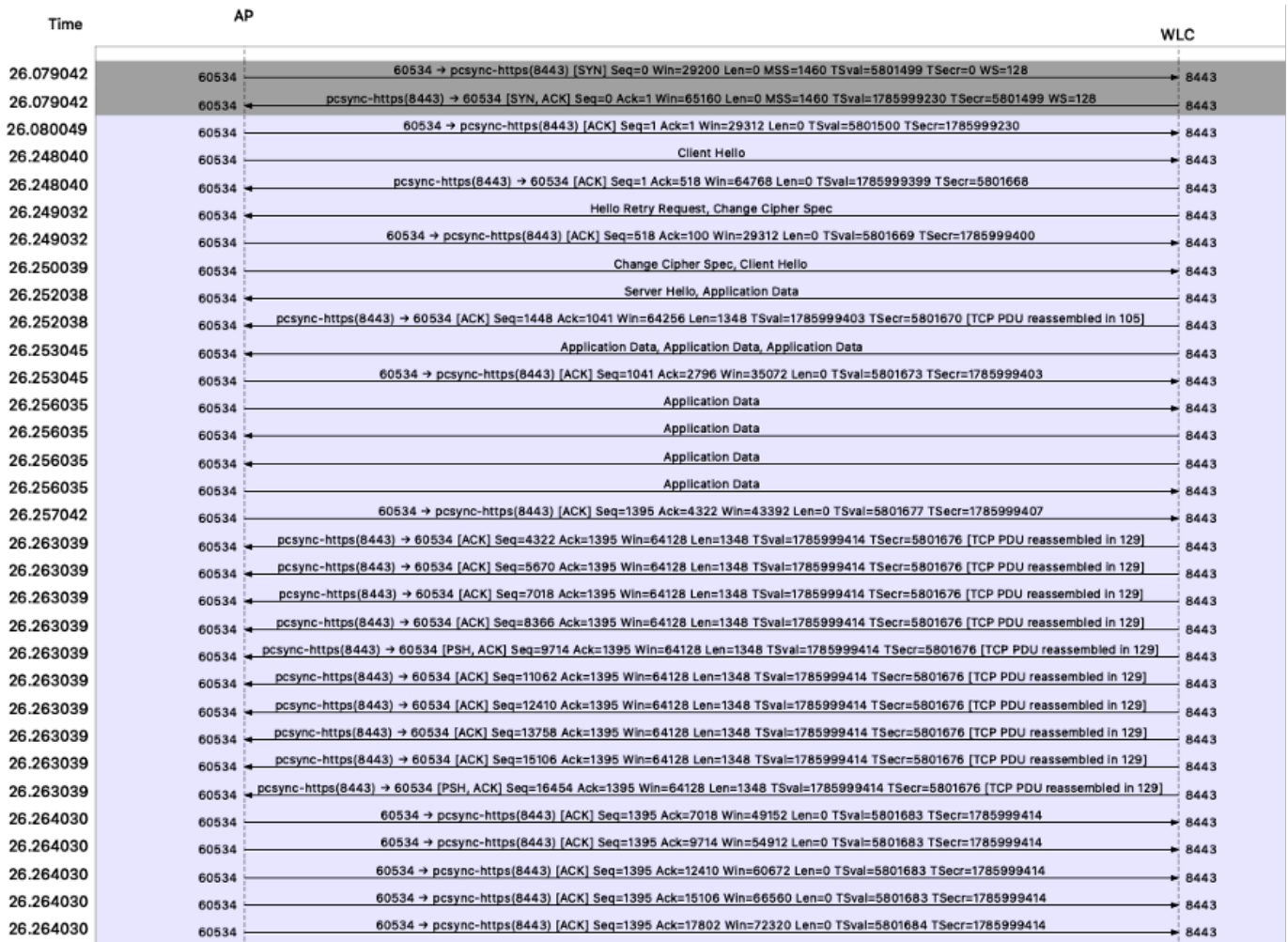
Anwendungsfall

Diese Methode eignet sich besonders für die Beschleunigung von AP-Image-Upgrades, insbesondere in großen Bereitstellungen oder an entfernten Standorten, wo die Latenz- und Bandbreitenbeschränkungen des CAPWAP-Steuertunnels herkömmliche In-Band-Downloads zeitaufwendig machen können.

Prozessübersicht

1. Das neue AP-Image wird auf dem WLC bereitgestellt.
2. Die Aktualisierungsmethode für OOB-HTTPs ist auf dem Controller aktiviert und konfiguriert.
3. Wenn der Access Point die OOB-Methode unterstützt, versucht er, das erforderliche Image vom nginx-Webserver auf dem Controller über HTTPs auf dem konfigurierten Port herunterzuladen.
4. Wenn die HTTP-Dateien erfolgreich heruntergeladen wurden, fährt der Access Point mit dem Upgrade-Prozess fort.
5. Wenn das Herunterladen der HTTPs fehlschlägt, greift der Access Point automatisch auf die standardmäßige In-Band-CAPWAP-Downloadmethode zurück.

Die Paketerfassung zeigt, dass der WLC als HTTP-Server und der AP als HTTP-Client fungiert und eine Standard-TCP-Verbindung über Port 8443 und den Dateidownload initiiert.



HTTPS-basierter Image-Upgrade-Paketfluss

Konfiguration (CLI)

<#root>

Enable the HTTPS upgrade method:

```
configure terminal
ap upgrade method https
end
```

Configure a custom HTTPS port (Optional - default is 8443):

```
configure terminal
ap file-transfer https port
```

end

Konfiguration (GUI)

1. Navigieren Sie zu Konfiguration > Wireless > Wireless Global.
2. Aktivieren Sie im Abschnitt AP Image Upgrade (AP-Image-Upgrade) die HTTPs-Methode.
3. (Optional) Geben Sie die Werte in das Feld HTTP-Port ein.
4. Klicken Sie auf Auf Gerät anwenden.

Überprüfung (CLI)

<#root>

show ap upgrade method

<- Check global HTTPS method status

show ap file-transfer https summary

<- View configured and operational HTTPS file transfer port

show ap name

config general | sec Upgrade

<- Check if a specific AP supports OOB capability (Look for "AP Upgrade Out-Of-Band Capability : Enabled")

show wireless stats ap image-download

<- View the method used for recent downloads (Check the Method column)

show platform software yang-management process

<- Verify nginx server status

Einschränkungen/Überlegungen

- Erfordert Cisco IOS® XE Dublin 17.11.1 oder höher.
- Nicht unterstützt von integrierten Cisco Wireless Controllern oder Cisco Wave 1 Access Points.
- Erfordert die Aktivierung der globalen HTTPS-Konfiguration auf dem Controller.
- Der nginx-Server muss auf dem Controller ausgeführt werden.
- Der konfigurierte Port muss zwischen dem Controller und den APs erreichbar sein.
- Das Upgrade kann fehlschlagen, wenn der HTTPS-Server-Vertrauenspunkt über eine Kette von Zertifizierungsstellenzertifikaten verfügt.
- Muss vor dem Downgrade auf Versionen vor Cisco IOS® XE 17.11.1 deaktiviert werden

(keine AP-Upgrade-Methode https).

- Port 443 ist reserviert. Vermeiden Sie andere Standard-/bekannte Ports.
- Standard-Port 8443-Konflikt: Wenn der HTTPS-Zugriff der Controller-GUI ebenfalls 8443 verwendet, müssen Sie einen anderen Port für die AP-Dateiübertragung oder den GUI-Zugriff konfigurieren.

Manuelles, individuelles AP-Upgrade über TFTP/SFTP

Diese Methode umfasst den direkten Zugriff auf die AP-CLI über die Konsole oder SSH und das Starten des Image-Downloads von einem TFTP- oder SFTP-Server. Dies ist nützlich, um bestimmte Access Points zu beheben, Access Points zu aktualisieren, die derzeit nicht mit einem Controller verbunden sind, oder um ein vom TAC bereitgestelltes Debugging-Image zu laden.

AP-Bild suchen:

Bei diesem Vorgang wird das AP-Image direkt auf den AP geladen. Bei einem WLC-basierten Upgrade wählt der WLC das richtige Image für den AP aus dem WLC-Image-Paket aus. Hier ist eine manuelle Auswahl erforderlich.

Die AP-Image-Version verwendet eine andere Namenskonvention als die WLC-Image-Namenskonvention.

Navigieren Sie zum Link [Unterstützte Access Points in den Softwareversionen der Cisco Catalyst Wireless Controller der Serie 9800](#).

[Unterstützte Access Points in den Softwareversionen der Cisco Catalyst Wireless Controller der Serie 9800](#)

Supported Access Points in Cisco Catalyst 9800 Series Wireless Controller Software Releases

Table 5. Cisco Catalyst 9800 Wireless Controller and Supported Access Points

IOS XE Release	Access Point Image Version Number	Access Point Release	Supported Access Points
Cisco IOS XE 17.17.1	17.17.0.87	15.3(3)JPV	Cisco Wireless Wi-Fi 7 APs: 9176 (I/D1), 9178I, 9172(I/H) Cisco Catalyst Wi-Fi 6E APs: 9136 (I), 9162 (I), 9164 (I), 9166 (I/D1) Cisco Catalyst Wi-Fi 6 APs: 9105AX (I/W), 9115AX (I/E), 9117AX (I), 9120AX (I/E/P), 9130AX (I/E) Cisco Aironet APs: 1815 (I/W/M/T), 1830 (I), 1840 (I), 1852 (I/E), 1800I, 2800 (I/E), 3800 (I/E/P), 4800 (I) Outdoor and Industrial APs: 1542, 1560, 1570, and IW3702 Integrated Access Point in Cisco 1100 ISR (ISR-AP1100AC, ISR-AP1101AC, and ISR-AP1101AX) Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point, Cisco 6300 Series Embedded Services Access Point, Cisco Catalyst 9124AX (I/D/E) Access Points, Cisco Catalyst 9163 (E) Series Access Points, Cisco Catalyst Industrial Wireless 9167 (I/E) Heavy Duty Access Points, Cisco Catalyst IW9165D Heavy Duty Access Points, Cisco Catalyst IW9165E Rugged Access Points Sensors: Cisco Aironet 1800s Active Sensor Pluggable Modules: Wi-Fi 6 Pluggable Module for Industrial Routers

Wireless AP-Kompatibilitätsmatrix

In der ersten Spalte wird das CCO-Image des 9800 WLC beschrieben. In der dritten Spalte sind die jeweilige Bildversion und in der vierten Spalte die unterstützten Access Points für diese Version aufgeführt. Angenommen, das AP-Image muss auf dem AP 9130 für Version 17.17.1 installiert werden. Wenn die Tabelle überprüft wird, lautet der Name des AP-Images 15.3.(3)JPV, und der 9130 wird als unterstütztes Modell aufgeführt.

Der nächste Schritt besteht darin, zu software.cisco.com zu navigieren und das Image aus dem Download-Ordner des Access Points abzurufen.

Downloads Startseite / Wireless / Access Points Catalyst 9130AX-Serie Access Points / Catalyst 9130AXI Access Point / Lightweight AP Software - 17.17.1(ED)

[Software-Download - Catalyst 9130AXI Access Point](#)

Software Download

[Downloads Home](#) / [Wireless](#) / [Access Points](#) / [Catalyst 9130AX Series Access Points](#) / [Catalyst 9130AXI Access Point](#) / [Lightweight AP Software- 17.17.1\(ED\)](#)

[Expand All](#) [Collapse All](#)
Latest Release
17.15.3(ED)
15.3.3-JPQ4(MD)
17.17.1(ED)
17.16.1(ED)

Catalyst 9130AXI Access Point

Release 17.17.1 **ED**

[My Notifications](#)

Related Links and Documentation
- No related links or documentation -

File Information	Release Date	Size
WIRELESS LAN LWAPP ap1g6a-k9w8-tar.17_17_0_87.tar Advisories	27-Mar-2025	89.49 MB

AP-Image-Speicherort



Warnung: Der Download-Pfad unterscheidet sich je nach AP-Modell und AP-Image-Version.

Prozessübersicht

1. Legen Sie die Ziel-AP-Image-Datei(en) auf einem zugänglichen TFTP- oder SFTP-Server ab.
2. Zugriff auf die AP-CLI (Konsole oder SSH)
3. Führen Sie den Befehl `archive download-sw` aus, und geben Sie den Server- und Image-Dateipfad an.
4. Der Access Point lädt das Image herunter.
5. Starten Sie nach Abschluss des Downloads den CAPWAP-Prozess neu, oder laden Sie den Access Point neu, damit das neue Image wirksam wird.

Konfiguration (AP-CLI)

<#root>

```
archive download-sw /no-reload tftp:///
```

<- Using TFTP:

```
archive download-sw /no-reload sftp:/// Username:
```

Password:

<- Using SFTP:

```
reload
```

<- Restart CAPWAP process after download:

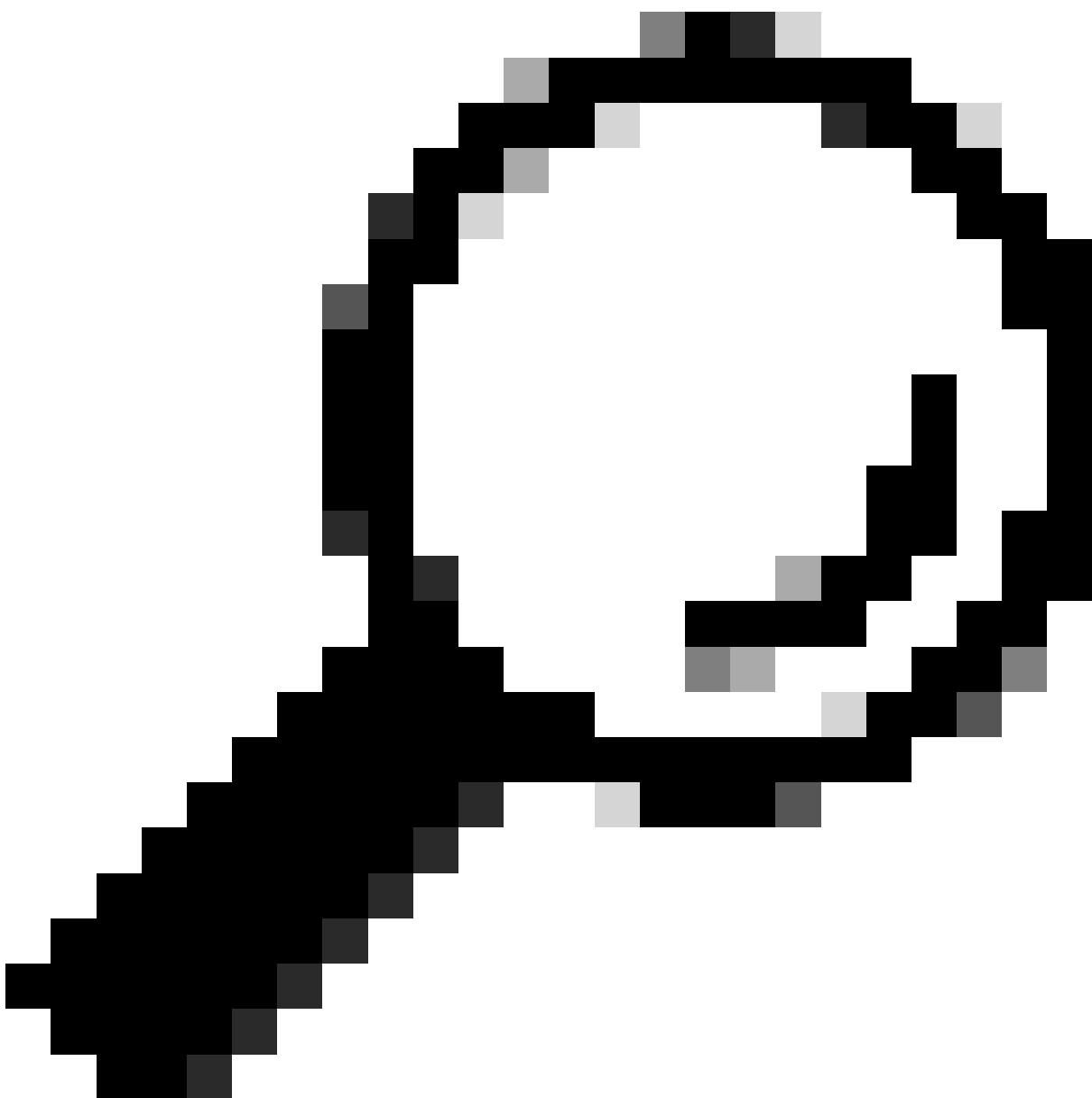
Verifizierung

- Überwachen Sie die TFTP-/SFTP-Serverprotokolle, um den Download zu bestätigen.
- Beobachten Sie den Fortschritt und den Abschluss des Downloads über die AP-Konsole.
- Überprüfen Sie nach dem Neustart/Neuladen die neue Image-Version auf der AP-CLI oder dem WLC.

Einschränkungen/Überlegungen

- Erfordert direkten CLI-Zugriff auf jeden Access Point.

- Nicht skalierbar für das Upgrade einer großen Anzahl von APs einzeln (Skripterstellung ist optional).
 - Die TFTP-Leistung hängt von der Latenz ab. SFTP (unter Verwendung von TCP) schneidet besser bei Pfaden mit hoher Latenz ab, erfordert jedoch eine interaktive Authentifizierung (Benutzername/Kennwort).
 - Die Übernahme/No-Reloading verhindert, dass der Access Point unmittelbar nach dem Download neu geladen wird, sodass der Neustart-/Reload-Zeitpunkt manuell gesteuert werden kann.
 - Wenn APs von AireOS auf 9800 migriert werden, wird empfohlen, den AP zunächst auf eine bestimmte AireOS-Version (8.10.190.0 oder höher) mit Fixes zu aktualisieren, bevor der 9800 hinzugefügt wird.
-



Tipp: WLAN Poller ist ein Tool, mit dem Sie Skripts erstellen können, um mehrere APs manuell zu aktualisieren. Suchen Sie den WLAN-Poller an diesem Standort. [WLAN-Poller](#)

Welche Methode für welche verwenden

- Für OEAPs oder Telearbeiter-APs über Verbindungen mit hoher Latenz:
Aktivieren Sie CAPWAP Image Download Time Enhancement. Dies wurde speziell entwickelt, um die CAPWAP-Leistung für diese Bereitstellungstypen zu verbessern, indem ein gleitendes Fenster verwendet wird, das das Latenzproblem innerhalb des CAPWAP-Frameworks direkt anspricht.
- Für FlexConnect APs in Zweigstellen mit begrenzter WAN-Bandbreite:
Nutzen Sie das Efficient Image Upgrade im FlexConnect-Modus. Diese Methode wird dringend empfohlen, da sie die WAN-Last erheblich reduziert, indem sie einen primären WAP für die lokale Verteilung über TFTP verwendet und so eine höhere interne Netzwerkgeschwindigkeit nutzt.
- Für APs im lokalen Modus (oder FlexConnect/OEAP, wenn die zuvor beschriebenen Methoden nicht anwendbar oder ausreichend sind) auf unterstützten Plattformen (Cisco IOS® XE 17.11.1+):
Ziehen Sie den Download des HTTP-basierten Out-of-Band-AP-Images in Betracht. Bei dieser Methode werden TCP/HTTPs für den Bulk-Transfer verwendet. Dies ist bei Verbindungen mit hoher Latenz effizienter als bei Standard-CAPWAP. Es bietet auch einen Fallback zu Standard-CAPWAP, wenn die OOB-Übertragung fehlschlägt.
- Für die Fehlerbehebung eines einzelnen Access Points, die Aktualisierung eines Access Points, der keinem WLC angehört, oder in Notfallszenarien:
Führen Sie ein manuelles individuelles AP-Upgrade über TFTP/SFTP durch. Dies ermöglicht die direkte Steuerung des Upgrade-Prozesses für ein bestimmtes Gerät, ist jedoch bei umfangreichen Bereitstellungen ohne Automatisierung nicht praktikabel. SFTP wird aufgrund der Verwendung von TCP im Allgemeinen gegenüber TFTP bevorzugt, um eine bessere Leistung gegenüber Pfaden mit hoher Latenz zu erzielen.
- Standard-CAPWAP-Upgrade: Obwohl es sich hierbei um den Standard handelt, wird er aufgrund des inhärenten Stopp-and-Wait-Mechanismus, der zu langsamen Übertragungen und möglichen Zuverlässigkeitsproblemen in älteren Versionen führt, nicht als primäre Methode für das Upgrade von Remote-Access Points über WAN-Verbindungen mit hoher Latenz empfohlen. Verwenden Sie nach Möglichkeit die für Remote-Standorte beschriebenen optimierten Methoden.

Wählen Sie die Methode aus, die am besten zu Ihrem AP-Betriebsmodus, den Netzwerkbedingungen, der WLC-Softwareversion und der Größe Ihres Upgrade-Vorgangs passt, um einen reibungslosen und effizienten Prozess für Ihre Remote-APs zu gewährleisten.

Schlussfolgerung

Während sich das standardmäßige CAPWAP-Image-Download-Verfahren für lokale Netzwerke eignet, profitieren Remote-AP-Bereitstellungen über WAN-Verbindungen erheblich von optimierten Upgrade-Techniken. Wenn Sie die Einschränkungen von Standard-CAPWAPs im Vergleich zu hohen Latenzzeiten verstehen, können Sie den richtigen Ansatz wählen. Die Verbesserung der CAPWAP-Image-Download-Zeit verbessert die Leistung für OEAP/Telearbeiter-APs, durch ein effizientes Image-Upgrade werden FlexConnect-Bereitstellungen durch eine Reduzierung der

WAN-Last optimiert, und Out-of-Band-HTTPs bieten eine schnellere Alternative für unterstützte Plattformen. Die manuelle TFTP/SFTP-Methode stellt nach wie vor ein nützliches Tool für die Fehlerbehebung und bestimmte Szenarien dar.

Referenzen

[Effizientes Image-Upgrade](#)

[Download von Out-of-Band-AP-Images](#)

[Beschleunigung des Herunterladens von AP-Images \(OEAP oder nur Telearbeiter\)](#)

[Unterstützte Cisco Access Points in Softwareversionen der Cisco Wireless Controller-Plattform](#)

[WLAN-Poller](#)

[Migration von AireOS WLC auf Catalyst 9800 mit WLANPoller](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.